Executive Summary

Information and Communication Technologies (ICT) Computer Systems' (CS) role is to design, procure, implement and maintain computer hardware, server software, IT security, data centers and database configurations for NMSU as an "always available" administrative service.

These include all computer servers (hardware, operating system, programming and authentication) supporting the primary business and administrative applications for NMSU. CS installs, configures, and maintains the databases that hold all of the business and administrative data for NMSU. We provide backup and recovery services for all administrative data and servers. This includes both primary and disaster recovery backups. We also provide server administration, database support and backup/recovery services to departments, colleges and branch campuses across NMSU, on a contract basis.

All of these services support instruction, research, and administration consistent with New Mexico State University's mission. CS supports the expectation to engage in learning activities and business, any time of the day or night whether on campus, from home or traveling, using information technology.

CS has primary responsibility for the two main NMSU email applications, email routing, virus and spam filtering and list server administration. Also CS builds the servers and configures and integrates the applications that make up the NMSU web presence and student webpage design and publishing environment. User authentication and shared data storage are also part of CS responsibility.

CS manages primary building monitoring and security for the Computer Center, Milton Hall data center and offsite storage. It also handles functional administrative enterprise security analysis, workflow and access control. CS coordinates and executes nightly process scheduling, management and monitoring. The main computer center, as well as backup computer centers and the shared server room, are designed and managed for secure access, power, cooling and humidity by CS.

CS coordinates IT Security for all NMSU campuses. This includes forensics investigations for crimes, policy violations or compromised systems. Additionally handling copyright violation, infected device notification, network blocking, system log aggregation and analysis, antivirus software management, vulnerability scanning and security planning and direction is the role of CS.

CS Consists of five departments, UNIX System Administration, PC System Administration, Database Administration, Information Security and Data Centers & Access Control.

CS regularly assesses both hardware and software assets to determine whether they still support the requirements of the university and are supported by the manufacturer/vendor.

Numerous internal licensing agreements for software packages, operating systems, more than four hundred servers and storage devices possibly directly affected by manufacturer/vendor “end of life” or “end of sale” designations are tracked.

A typical hardware asset passes through several milestones as it moves out of the marketplace. The first is the End of Life announcement, which is an alert that the manufacturer will begin phasing out a given product or platform. Next are End of Sale, End of Engineering and End of Support milestones. These milestones differ between product lines, but generally follow a schedule such that the End of Support falls about three years after the End of Sale date. In order to plan each product has to be considered separately.

Computer technology changes quickly. ICT has always had the philosophy of leading edge not bleeding edge. Overly aggressive plans face the danger of picking the non-prevailing technology and overly conservative plans risk technology obsolescence early or even before project completion. Changing technologies must be monitored to ensure that ICT technical plans contain appropriate balance aligned to NMSU strategic initiatives with broader IT trends. These trends are identified by EDUCAUSE, Gartner and other IT industry advisers, to ensure that NMSU’s technological resources stay current, foster innovation, and support the University’s mission.

An example of a recent emerging technology is cloud computing. NMSU now uses cloud computing for several services including the MyNMSU portal, CASHNet, Live at EDU email, Canvas learning management system, People Admin, Hobsons Apply and others.

Major server, software and storage upgrades provide better server availability and responsiveness, increased storage capacity and enhanced security to administrative applications. NMSU must continue to update its IT infrastructure to be able to offer the quality and quantity of services expected of a modern university system. This will ultimately translate into a better computing experience for NMSU Faculty, Staff and Students as well as increased retention and recruitment.

As a result of ongoing security threats, CS must continue to develop and enhance its information security capability to monitor and manage security at the institution, while balancing the needs of and employees and students throughout the NMSU system.

Explosive growth in the use of information technologies as the basis for institutional communications, information processing and data exchange comes at a time when there are an increasing number of security threats. These include viruses and worms designed to propagate through networked client and server devices. Hackers are able to break into servers, desktops, tablets and even cellphones that are not aggressively maintained with the latest updates and security patches.

In addition NMSU must continue to develop and understand where its institutional data resides, who is allowed to access that data and by what means. Just seven years ago

NMSU had four central and a handful of satellite administrative systems. Most of these were accessed by a terminal application on a desktop. Today there are more than eighty applications with capabilities to access and store data available through and on the web to any imaginable device. Data access and security policies must continue to be developed and augmented to meet the ever changing technological landscape.

Additionally, compromised systems can be used to launch a variety of attacks that threaten the integrity and usability of the Internet. ICT and other NMSU technologists must apply appropriate security measures in a timely manner. Intrusion and prevention detection capabilities must be developed and deployed. Security tools must be implemented and updated on a regular basis. Logs and reports must be monitored and acted upon. Entire networks comprising administrative hardware and applications must be scanned for vulnerabilities regularly.

Key Objectives:

1) Deploy more and better *internal* cloud computing capabilities through the use of hardware virtualization for increased system availability, performance and energy efficiency.
2) Provide software and hardware tools to support the build out of the Information Security group to address the increased need to monitor regulatory compliance, detect malicious activity, manage data policy enforcement, oversee External Cloud Computing Security initiatives and develop, maintain and enforce risk based "best practices" security procedures at NMSU.
3) Replace existing data storage hardware with next generation data storage, including virtualization and solid state, to insure continued system reliability and performance.
4) Upgrade existing data backup server and storage hardware with next generation hardware to meet both near and geographically remote backup requirements.
5) Develop robust disaster recovery capabilities including existing fiber resources on the Rio Grande Corridor allowing for the deployment of redundant servers, storage and backups at a geographically remote sister sight.
6) Modernization of the primary data center to use alternative cooling and power savings technologies to help NMSU reduce its carbon foot print while continuing to provide an environment for all institutional computing needs.
7) Relocate the secondary data center out of the Milton Hall basement switch room.

Why Invest?

An annual capital investment allows ICT to target services in most need of enhancement, elimination or replacement, and to reduce near term exposure and risk. A capital investment plan will refresh the technology and decrease operational deficiencies.

NMSU's technology must evolve and keep pace with technological advances in order to continue to provide the services users within the university need to provide the basis for delivering new services in the future.

When equipment is purchased it is consistent with industry standards and practices, and represents the most practical advanced technology available. The pace of technology improvement has quickened and the goal is to get the most of our hardware and software purchases but to only change technology when it represents a clear technological advancement, needed performance increase or reliability improvement for NMSU.

Information Technology is critical to the university and fundamental to the success of administration, research, teaching, and learning. The goal of ICT Computer Systems is to continue providing seamless, pervasive and exceptional services for the university community.

Five year plans and IT, a caveat

Given the rate of change in IT, as articulated above, it is almost impossible to say "**how**" technology services will be delivered in five or even three years.

The NMSU Learning Management System began as a non-critical application running on an office desktop in 2003. By 2012, after five technology enhancements it had become a mission critical service requiring 34 physical servers, high availability and located in two buildings for disaster recovery. Today, the number of servers has grown to more than 200 servers, but these servers can be run as virtual servers. Using virtualization technology requires fewer numbers of servers called hypervisors and some can be run entirely in the cloud.

It is also hard to determine "**what**" new services and current services will be needed and will their delivery change in importance.

The network service is a great example of this problem. Since the beginning every device accessing the internet had to connect to a wall jack. But since2010 demand for wireless access to the internet has outstripped any predictions made due to the growth in the number wireless devices students and faculty now use. The new service is wireless internet access. It is new because it exists in addition to wired services and has a totally different hardware, deployment strategy, security concerns and cost.

It is extremely difficult to predict, accurately, more than two years in advance. In three years a new technology not yet invented or matured could become a requirement for NMSU. The good thing is it will likely require ICT to do something different but familiar with network, storage and servers.

Risk to capital investment

Each piece of very complex hardware or software purchased by NMSU requires a human to install, configure, customize, monitor and upgrade it on a regular basis. For NMSU to get the most out of each purchase, the human must become intimately familiar with the

technology. It is also likely that the human will be sick from time to time, so a backup person with some knowledge of the technology is a must.

Since the implementation of Banner in 2005 ICT has dropped 13 FTE. Yet it manages and maintains ten to twenty times the number of servers, switches and software.

NMSU, as an institution, is risking its' investment of capital funds and ultimately its' security if it does not begin to invest in and competitively compensate IT staff positions to fulfill the needs of the institution.

Technical Description

This section contains an overview of the building blocks of hardware and software used to deliver services in CS.

Data Centers and Hardware
The main ongoing data center expenditures are due to providing redundant and smoothed power. CS currently maintains seven Uninterruptible Power Supply (UPS) systems of various sizes. Each system requires that all batteries be cyclically replace every five years.

The data center also runs a towable generator to power the network in the case of a simultaneous outage of the Cogeneration Plant and El Paso Electric or the failure of switching gear between two. This device could require replacement in the next 5 years.

NMSU needs a geographically remote "hot" data center. The current secondary datacenter and offsite backup storage site are all a few tenths of a mile from each other in the same flood plain. In the event of a disaster the chances of all sites being affected is high. NMSU drives tapes offsite to Alamogordo, however the data can be up to a week old. Without a hot sight, recovery would take at least 30 days. Best practice disaster recovery site separation is 50 miles. Five Tributary Adapter Modules: TAMs are required to make Rio Grande Fiber usable by CS for remote failover databases and backups at a geographically distant site.

As soon as possible a new site built secondary datacenter should be constructed to move all failover and development servers, databases, switches, routers, VOIP hardware and central storage out of the NMSU switch room in the basement of Milton Hall.

Computer Hardware and Software
ICT has been taking advantage of Computer Virtualization for years. It combines a highly specialized operating system (VMWare) with high performance computers having numerous computing cores and large amounts of storage and memory. They are used to host software applications that previously ran each on their own individual physical server. This strategy has allowed ICT to eliminate more than forty physical servers and storage devices from our data center and consolidate more than fifty applications onto just four server pairs. These once single-point-of-failure services are now designed to migrate to a failover server in the secondary data center in the event of a hardware or

facilities failure in the primary data center. In addition to better availability, NMSU saves in cooling generation and electricity consumption costs. Also as new software services are needed anywhere in the institution, they can be deployed on existing virtual server capacity.

ICT will need to purchase additional virtual server hardware pairs to continue to virtualize the remaining aging computer hardware running enterprise and departmental applications as well as meeting the new needs of the institution.

Licensing capacity for VMWare will also be needed.

ICT must, on a three to five year cycle, purchase hardware to replace aging hardware running enterprise database applications for Banner and Banner ODS physical servers.

Additionally, newer upgraded versions of enterprise software tend to be more robust from a functional standpoint. This usually leads to an increase in capacity needs or outright change in architecture requirements. This translates to a year to year requirement for more hardware resources.

Additionally there is a periodic need to replace or augment specialized standalone physical servers like backup, monitoring and data servers.

Storage Hardware and Software

ICT deployed its first Storage Area Network (SAN) in 2005 when NMSU began to deploy SCT Banner. A SAN has three main components.

The "N" is a separate network that is used by servers to communicate with storage. The network has switches and communication cards that periodically need upgrading for number of ports and speed.

The "S" is storage and is composed of controllers that talk to large banks of disk drives of various size and performance capabilities.

While "A" for area is not really a component I use it to represent the fiber connections needed between the physical locations of the storage and the servers and that ultimately make up the networks functionality.

ICT currently has over 500 Terabytes (TB) of central storage connected to the SAN. Half of this storage is over six years old. ICT will be looking at next generation storage in the 2020 fiscal-year.

Additionally the rate of data growth for storage is currently holding steady and 50TB per year. Attaching new storage consumes ports and may require network fiber enhancements for speed or increase paths.

Managing this amount of storage for performance and growth is time consuming and complex. It requires licensing specialized virtualization hardware and software.

This constant need for more storage infrastructure will require a commitment to ongoing, regular, fiscal supplements.

ICT have be purchasing solid state storage to attach to the SAN to increase enterprise application performance. SSD is extremely fast storage built from memory chips as opposed to conventional disk drive technology. It is used to alleviate processing bottlenecks and ultimately reduce overall time to complete long running tasks.

Backup/DR Hardware and Software

ICT has been running a tape library and upgrading it in place since 2005. It started out with six low density tape drives which we have upgraded over the years to sixteen drives capable of using tape four times as dense. We plan to continue to increase the number of drives and their capacity as well as the tape capacity of the library. Though tapes lack the glamor of other backup technologies they are the foundation of a tiered backup strategy, very reliable and inexpensive to operate.

ICT purchased a Virtual Tape Library in 2008 with 40 TB of space. This device emulates tape storage but is actually disk based. It has faster performance and uses specialized software to compress and de-duplicate the data being backed up. Today, we have increased capacity to more than 120 TB.

This device is going off support in June of 2014. We have already purchased some next generation VTL components but will need to replace 80 to 100 TB, based on needs, by next year.

ICT uses Tivoli Storage Manager backup software. We purchased a five year license last year. The license is capacity based so will require periodic "true up" expenses.

Security Hardware and Software

ICT runs the large NMSU regional network with five campuses and extension offices. It has over 300 administrative servers or as hackers like to refer to them, targets. There are over twenty thousand unique devices connecting to the network and soon five thousand simultaneous wireless network connections. Information Security works with the Networking Group to try to secure this network.

In the next two years NMSU needs to quickly develop a proactive risk based security program. This will require ICT to develop a comprehensive IT security implementation plan. This is a must to not only to reduce risk to NMSU, but to meet the regulatory requirements of institutions of higher education.

Some of the first action items from this plan will be an institutional data inventory audit project to determine where university data is located, where it should be kept and how it

should be accessed. This project will require the university wide licensing of Data Auditing Software.

NMSU currently licenses antivirus software which requires periodic renewal.

Regulations for encrypted data storage requirements will dictate the need for licensing and maintenance of security key management and encryption software.

As NMSU deploys more web based applications it will need to become a web certification authority by partnering with a company to provide this service. This strategy will save money and increase flexibility.

Also develop institution wide IT security policy, procedures, guidelines and training programs. ICT has partnered with NMSU Training Services to develop security training. It will also need to purchase supplemental online training software licenses for staff and students.

Since NMSU has three cloud computing applications with more to come, ICT needs to formalize comprehensive cloud computing contract policy.

Information security needs to fingerprint our normal network activity and ramp up continuous network monitoring to enable us to proactively protect our resources. This is done through the use of hardware appliances, servers and software that are both highly specialized and customizable.

Servers, switches and router hardware as well as web and application software all produce logs of the activity they carry out. NMSU has in excess of 2500 such devices each producing hundreds to thousands of lines of logs per day. Analysis of log data to detect attacks and compromised systems require high speed storage and hardware as well as specialized software. Security best practices dictates that this data be examined on a regular basis.

In order to reduce the risk of data loss, access to a number of computer services and enterprise applications will require the use of a virtual private network (VPN). The current VPN at NMSU is at capacity, slow and outdated. Security best practices require NMSU have the capability to restrict access to select services using VPN technology

NMSU needs to develop and deploy an Identity Management IdM strategy across the institution. One of the biggest risk factors for data loss is unauthorized access. This occurs due to the lack of a universal account access management process. The solution is to implement a system that automatically provisions, modifies and de-provisions access, based on the position title/role(s) of a person or a group, using the rules established by the data custodian responsible for the access. This system will reduce risk, improve efficiency as well as unify policy across many disparate systems.

To implement this NMSU will need to purchase a product that best meets our needs.

Database Software
The Database's main focus is database performance, tuning and upgrading as well as Banner upgrades and the oracle application services front end to the database.

Their main expense going forward would be software to help with performance monitoring and upgrade/release tracking.

Capital Expenditures

The following capital requests represent the five year capital outlay plan for the NMSU Las Cruces campus. The Las Cruces campus serves as the system office for the main campus as well as the NMSU community colleges for the Learning Management System (CANVAS), Enterprise Resource Planning (Banner), reporting (COGNOS), email (Office 365 and local exchange), Help Desk, Portal (MyNMSU), networking and many other services. This request is part of a bigger over arching plan that takes into account other funding sources in order to maintain effective IT services at NMSU.
There is a certain amount of hubris involved in predicting Information Technology (IT) capital needs out past two years due to the rapid change in, and adoption of, technology by students and faculty. This is still a good planning tool, however as more IT services begin to be hosted in the cloud, funding and service methodologies will have to be adapted to meet this new reality.
As a result of the downward trend in state revenue over the last decade, it should be realized that NMSU continues to defer the implementation of IT resources that are expected of a tier one research institution. If we continue to defer it will impede the ability to deliver on the core mission of secure, timely and effective pedagogy and research. As technology becomes more critical to business of the university and if technology is not updated, it will make NMSU less capable of attracting and retaining students, as well as talented faculty and staff.

2020-2021

Computer Hardware and Virtual Servers - Replacement & Growth	$200,000.00
Disk space for the Storage Area Network	$250,000.00
Disaster Recovery (Backups) replacement	$348,000.00
Long Distance/Short Distance Fiber Routing Equipment (DWDM)	$248,000.00
Fiber and Trenching	$50,000.00
Network Router and Switches for local and remote Data Centers	$200,000.00

(Industry average replacement is 10 years)

Security/Firewall Appliance - Upgrade	$120,000.00
Vulnerability Monitor/Testing and IDS/IPS (Intrusion Detection/Protection System) Appliance	$100,000.00
Total	$1,516,000.00